La notion de "donnée à caractère personnel" a-t-elle encore un sens dans la protection des données de communications électroniques ?

Rosier, Karen

Published in:
Law, norms and freedom in cyberspace = Droit, normes et libertés dans le cybermonde

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 12
La notion de « donnée à caractère personnel » a-t-elle encore un sens dans la protection des données de communications électroniques ?

Karen ROSIER*

CHAPITRE 1. La protection des données de communications électroniques entre deux règlementations

1. Le droit de la protection des données est en pleine mutation. Sous les feux des projecteurs de façon assez inédite alors qu'il existe depuis des décennies, il remet en question des pratiques développées par les grands acteurs des technologies de l'information. On pense en particulier au *big data*. De longue date, l'internet ne sert plus uniquement à interconnecter. Il permet de collecter des données, de suivre des internautes dans le comportement de navigation électronique et d'utiliser ensuite ces données, notamment pour constituer des profils de consommations, des schémas de comportement, etc. Là où le Règlement général sur la protection des données (RGDP)[1] s'attache à établir un rééquilibrage entre les droits des personnes concernées et les exploitants de ces données, on peut se demander quel sera l'apport de la règlementation sur les communications électroniques à cette entreprise.

* Maître de conférences à l'Université de Namur, chercheuse au Centre de Recherche Information, Droit et Société (Crids), Université de Namur et avocate (Versius).

[1] Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

En effet, 2018 sera une année phare dans ces deux domaines. Le RGPD déjà en vigueur entre en application le 25 mai 2018. Parallèlement à cela, une Proposition de Règlement ePrivacy est sur la table[2].

2. Le droit à la protection des communications est inscrit à l'article 9 de la Charte des droits fondamentaux de l'Union européenne. Les communications électroniques sont régies par un cadre de règlementation spécifique qui se situe à la croisée de deux pans de la législation : la protection des données et les services des communications électroniques.

La directive 2002/58/CE[3], modifiée quelques années plus tard par la directive 2009/136/CE[4], faisait partie d'un paquet de cinq directives et d'une décision destiné à reformer le cadre réglementaire régissant les services et réseaux de communications électroniques dans la Communauté.

Résolument ancrée dans cette règlementation sectorielle auquel elle emprunte des définitions de concepts clés de son régime juridique, la directive constitue, dans le même temps, une réglementation spécifique qui complète la directive 95/46/CE pour ce qui concerne les traitements effectués dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté.

3. Cette règlementation est en passe d'être modifiée. Comme déjà mentionné, une proposition de Règlement ePrivacy a été publiée le 10 janvier 2017[5], qui est censée à terme remplacer le régime façonné par ces directives.

---

[2] Proposition de Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM(2017) 10 final.

[3] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques). Cette directive remplace la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

[4] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

[5] Proposition de Règlement du parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM(2017) 10 final.

Le texte étant toujours en discussion et susceptible de modifications, je n'en évoquerai, sans prétendre être exhaustive, que certaines grandes lignes sans garantie que celles-ci soient maintenues dans le texte définitif[6]. Le propos se limitera en effet à quelques questions choisies par rapport au texte en projet en lien avec son interaction avec le RGPD. Ces questions se veulent le prolongement d'autres réflexions sur la législation existante. Le hasard veut que mes premiers pas en tant que chercheuse sous la supervision de Yves Poullet au sein du CRID aient eu lieu au moment où l'on découvrait le texte de la directive 2002/58/CE et que c'est ce texte qui m'ait inspiré ma première publication[7]. S'en sont suivi des discussions nourries avec Yves Poullet au fil des ans et des publications que nous avons rédigées sur ce sujet[8]. C'est tout naturellement que ce sujet m'a paru opportun pour lui rendre hommage. Quoi de plus indiqué, en effet, que de se fendre de quelques réflexions prospectives sur l'avenir de la protection des données de communications pour saluer en toute humilité un penseur du droit des technologies de l'information et de la régulation[9].

Et matière à réflexion il y en a me semble-t-il, dès lors que l'évolution qui se dessine en la matière nous éloigne à la fois d'un ancrage protection des données relatives à des personnes physiques et du giron des services de communications électroniques.

CHAPITRE 2. La protection des données de communications électroniques en mode hybride

4. Tant les directives 2002/58/CE et 2009/136/CE précitées vis-à-vis de la directive 95/46/CE, d'une part, que la Proposition de Règlement

[6] La proposition a d'ailleurs fait l'objet de plusieurs avis qui préconisent des améliorations du texte, que ce soit à l'initiative du Contrôleur européen de la protection des données (Avis 6/2017 sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement « vie privée et communications électroniques ») ou du Groupe de l'Article 29 (Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) du 4 avril 2017, WP 247).

[7] J. Dhont et K. Rosier, « Directive vie privée et communications électroniques : premiers commentaires », *Revue Ubiquité (R.D.T.I.)*, 2003, pp. 7-46.

[8] A Dix, K. Rosier et Y. Poullet, « Commentary on the Directive 2002/58/EC on privacy and electronic communications », *in Concise European IT Law*, Kluwer Law international, 2006, pp. 145-204, mis à jour en 2010.

[9] Et de l'autorégulation, de la corégulation (approches « *bottom up* » et « *top down* »), de la *soft law* qui ont fait suer nombre d'étudiants du cours de Sources et principes du droit pour lequel j'ai eu l'immense privilège d'assister Yves pendant une dizaine d'années. « Vive SPD !, Vive Toi !», pour reprendre une de ses expressions favorites.

ePrivacy vis-à-vis du RGPD, d'autre part, s'affirment comme *lex specialis*. On aurait tendance à en déduire qu'elles vont régir le traitement d'un certain type de données à caractère personnel, liées aux communications électroniques. Ce n'est pas aussi simple.

La première raison en est un mélange de concepts qui nuisent à la bonne compréhension de son champ d'application. Cette règlementation s'inscrit dans cadre sectoriel qui utilise d'autres concepts et d'autres critères d'application et qui balaie toute référence aux notions clés de la règlementation de la protection de la vie privée. Ainsi, la directive 2002/58/CE use de définitions propres pour viser les données concernées par les traitements (les données relatives au trafic ou les données de localisation[10]), sans inclure dans cette définition de référence au fait qu'il s'agit de données *à caractère personnel*. Elle vise comme destinataires des règles édictées les fournisseurs de services de communications électroniques sans préciser qu'ils ne sont visés que pour autant qu'ils aient la qualité de responsable de traitement au sens de la directive 95/46/CE. Il est également question, pour les actes décrits à l'article 5, § 3, de la directive 2005/58/CE, qui concerne notamment l'usage de cookies, du « stockage d'informations, ou [de] l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal […] » et non de *données à caractère personnel*. La directive 2002/58/CE va même jusqu'à prévoir une disposition protégeant les personnes morales[11] alors que la règlementation s'applique exclusivement à la protection des données relatives à des personnes physiques.

Si la directive 2002/58/CE entend indubitablement régir le traitement de données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté[12], les concepts utilisés ont donc de quoi semer le doute. En réalité, la directive ne se focalise pas exclusivement sur le traitement des données. Il est également question d'assurer la confidentialité des communications et, dans une certaine mesure, de prendre en compte les intérêts des personnes morales à voir certaines de leurs données protégées.

Le caractère hybride de cette règlementation est d'ailleurs flagrant lorsqu'on a égard à la loi belge qui a transposé la plupart des dispositions de la directive 2002/58/CE. En effet, ce n'est pas dans la loi relative à la protection des données du 8 décembre 1992 que cette directive a été transposée mais dans la loi du 13 juin 2005 relative aux communications électroniques. Et cette loi, son champ d'application, ses définitions

[10] Art. 2, b) et c) de la directive 2002/58/CE.
[11] Art. 13, 5 de la directive 2002/58/CE.
[12] Voy. art. 1er de la directive 2002/58/CE.

sont ancrés dans le contexte des communications électroniques. On y intègre une dimension protection des données tout en renvoyant au sein de certaines dispositions à la loi du 8 décembre 1992. Par le prisme de la transposition nationale, on a par ailleurs quelque peu modifié la portée de certaines dispositions. Il a été par exemple question d'opérateurs qui faisaient référence à des personnes qui fournissent ou revendent en leur propre nom et pour leur propre compte des services ou de réseaux de communications électroniques. Cela englobait d'autres acteurs que les fournisseurs de services de communications électroniques visés dans les définitions de la directive[13].

Tout cela est en passe de changer avec l'adoption d'un Règlement ePrivacy. Si celui-ci est adopté, il sera d'application directe et devrait logiquement supplanter les définitions nationales, mais uniquement pour ce qui concerne ce qui relève de son champ d'application (et donc pas forcément l'ensemble de la règlementation qui a trait au secteur des communications électroniques).

La question du champ d'application matériel et personnel se pose à nouveau par rapport à cette proposition de Règlement et on constate un détachement des critères d'application de la règlementation sur la protection des données.

5. Tout d'abord, la proposition de Règlement adopte une approche qui peut paraître ambigüe concernant la place laissée à la notion de donnée à caractère personnel.

L'article 4, 1), du RGPD définit la notion de données à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") » tout en précisant que « est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité

[13] Art. 2, 6°, et 9 de la loi du 13 juin 2005. L'article 8 de la loi du 31 juillet 2017 portant des dispositions diverses en matière de communications électroniques a toutefois modifié la loi pour ne viser que les personnes qui fournissent des services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques, ce qui réconcilie la règlementation nationale avec le champ d'application de la directive 2002/58/CE. L'exposé des motifs de la loi reconnaît d'ailleurs que la révision de la loi s'impose notamment en ce que la loi belge s'écartait de la directive (projet de loi portant des dispositions diverses en matière de communications électroniques, *Doc. parl.*, Ch. repr., n° 54-2558/001, p. 16).

physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Il y a donc à tout le moins deux éléments clés. D'une part, le fait que la donnée concerne une personne physique et, d'autre part, un lien entre ladite information et cette personne. Sur ce deuxième point, rappelons que le RGPD opère une modification par rapport à la directive 95/46/CE en intégrant l'idée qu'il n'est pas nécessaire qu'on puisse connaître l'identité de la personne pour qu'il soit question de données à caractère personnel : peut suffire la circonstance que cette personne est « individualisée ». Sans savoir qui est la personne concernée, on peut l'identifier dans la masse des individus par d'autres facteurs ou données recueillies[14]. Cet élargissement de la notion de donnée à caractère personnel participe d'ailleurs à une évolution du nouveau Règlement qui entend davantage protéger les individus contre le profilage et le ciblage via notamment la collecte d'informations sur Internet. Il est essentiellement question à l'heure actuelle de publicités comportementales qui visent à proposer des publicités ou des informations ciblées suivant un traitement de données associées à une personne individualisée (« *singled out* » pour reprendre la terminologie anglaise du RGPD). L'utilisation d'un cookie peut par exemple aider à cette individualisation en associant des requêtes de pages web à un identifiant unique qui permettra à la société qui a déposé des *cookies* de faire un lien entre cet identifiant et d'autres données générées par la navigation sur Internet.

6. J'identifie une modification dans la Proposition de Règlement ePrivacy dont la portée véritable pose question. Il est précisé à propos de l'opportunité de maintenir, tout en le révisant, un texte européen dédié aux communications électroniques que : « Tandis que le RGPD garantit la protection des données à caractère personnel, la directive "vie privée et communications électroniques" préserve la confidentialité des communications, lesquelles peuvent aussi contenir des données à caractère non personnel et des données relatives à une personne morale. Par conséquent, un instrument distinct devrait assurer une protection efficace de l'article 7 de la Charte »[15]. On en déduit que la règlementation doit avoir une portée plus large que le traitement de données à caractère personnel lié à la fourniture d'un service de communications électroniques.

[14] Voy. consid. 26 du RGPD.

[15] *Cf.* pt 3.1 de l'Exposé des motif de la Proposition de Règlement du parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM(2017) 10 final.

Cela ne se reflétait pas dans la définition du champ matériel de la directive 2002/58/CE. L'article 3 de la directive précise que « [l]a présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté […] ».

On ne peut manquer de constater que la définition du champ d'application matériel de la proposition de Règlement ePrivacy supprime les termes « à caractère personnel » et fait référence au traitement des données de communications électroniques et aux informations liées aux équipements terminaux des utilisateurs finaux. Le champ d'application du futur règlement est, pour l'heure, voué à être défini comme suit : « Le présent règlement s'applique au traitement des données de communications électroniques effectué en relation avec la fourniture et l'utilisation de services de communications électroniques dans l'Union et aux informations liées aux équipements terminaux des utilisateurs finaux[16] ».

La proposition de Règlement affiche clairement l'intention d'inclure, lorsqu'elle utilise les termes « données de communications électroniques »[17], à la fois le contenu de la communication[18] et les métadonnées, à savoir les données générées par celle-ci pour les besoins de la transmission[19]. La notion de données de communications électroniques est donc elle aussi exempte de toute allusion à la qualité de donnée *à caractère personnel*.

Il n'est pas aisé d'en tirer des conséquences claires. Le Groupe de l'Article 29 et le Contrôleur européen pour la protection des données qui ont commenté les dispositions de la proposition du Règlement n'épinglent pas cette modification. Il est davantage question de préconiser un alignement du niveau de protection exigé concernant les métadonnées et

[16] Art. 2, § 1er, Proposition de Règlement ePrivacy.

[17] Définies comme les « données de communications électroniques » le contenu de communications électroniques et les métadonnées de communications électroniques » (Proposition de Règlement ePrivacy, art. 4, k).

[18] Définies comme « le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son » (Proposition de Règlement ePrivacy, art. 4, l).

[19] Définies comme les « les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication » (Proposition de Règlement ePrivacy, art. 4, m)).

le contenu des communications électroniques[20], sans s'étendre sur le fait que ces données doivent ou non répondre à la qualification de données à caractère personnel. Dans le même temps, le Groupe de l'Article 29 se félicite de la suppression de certaines dispositions de la réglementation actuelle qui sont susceptibles de faire double emploi avec le GDPR. On pense en particulier au retrait des dispositions relatives aux obligations en cas de violation de données introduites par la directive 2009/136/CE et qui reçoit une consécration dans le GDPR puisqu'elles sont désormais imposées à tout responsable de traitement et non plus aux seules personnes visées dans la directive vie privée et communications électroniques[21]. Or cette obligation de notification ne sera applicable que lorsque l'on aura affaire à des données à caractère personnel.

7. Un deuxième point d'interrogation peut être ajouté concernant le champ d'application du futur Règlement ePrivacy. Il est certain que ce Règlement ePrivacy entend ne pas se cantonner à la protection des personnes physiques mais également intégrer une protection au bénéfice des personnes morales.

Une prise en considération des personnes morales existait déjà sous l'empire de la directive 2002/58/CE mais il s'agissait surtout, au travers de dispositions de la directive, d'inviter le États à assurer la protection d'intérêts légitimes des personnes morales lors de la transposition de la directive dans le droit national. Concrètement, cela était limité à la problématique des communications électroniques non sollicitées et des annuaires[22].

Pour se référer aux personnes qui bénéficient d'une protection dans la Proposition de Règlement ePrivacy, on quitte la définition de données à caractère personnel pour passer dans le champ terminologique du secteur des communications électroniques. La proposition de Règlement renvoie en effet aux définitions prévues dans le futur Code des communications électroniques européen présenté en septembre 2016[23]. L'article 2, 13), de ce Code encore à l'état de proposition définit, en maintenant les définitions actuelles, l'utilisateur comme « une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public » et l'article 2, 14), l'utilisateur final, comme « un

[20] Avis 6/2017 sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement « vie privée et communications électroniques »), p. 33 ; Groupe de l'Article 29, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) du 4 avril 2017, WP 247, pp. 13-14.

[21] Art. 34 du GDPR.

[22] Voy. art. 12 et 13 de la directive 2002/58/CE.

[23] Voy. Proposition de directive du parlement européen et du conseil établissant le code des communications électroniques européen, COM(2016) 590 final.

utilisateur qui ne fournit pas de réseaux de communication publics ou de services de communications électroniques accessibles au public ».

On en déduit que tout utilisateur final, qui peut être une personne morale ou une personne physique, bénéficie de la même protection. Ainsi le Groupe de l'Article 29 relève-t-il que les autorités de contrôle seront compétentes si des communications électroniques d'une personne morale devaient faire l'objet d'un suivi illicite[24].

La réglementation est donc appliquée sans qu'il ne soit nécessaire que les données se rapportent à une personne physique, alors qu'il s'agit d'un facteur clé de la délimitation du périmètre de la règlementation sur les données à caractère personnel. Cela pose la question de savoir si dès lors qu'on a affaire à une donnée de communications électroniques, peu importe si elle a trait ou non à une personne physique, les dispositions du futur Règlement ePrivacy ont vocation à s'appliquer.

Il est par ailleurs précisé dans le troisième considérant de la Proposition de Règlement ePrivacy que « [l]es données de communications électroniques peuvent aussi révéler des informations concernant les personnes morales, telles que des secrets d'affaires ou d'autres informations sensibles ayant une valeur économique. Aussi les dispositions du présent règlement devraient-elles s'appliquer à la fois aux personnes physiques et aux personnes morales ».

Cela me semble susciter deux questions. La première est de déterminer si, derrière cette volonté d'extension de la protection, il s'agit de protéger *toutes les données de communication* des personnes morales. La seconde concerne les conséquences de l'application des dispositions du futur Règlement ePrivacy à des personnes morales : cela entraine-t-il, pour ces personnes, le bénéfice des dispositions du RGPD ?

8. Concernant la première question, le troisième considérant de la proposition de Règlement laisse entendre qu'il s'agit d'une extension assez générale de la protection aux personnes morales. Il précise que « [l]e présent règlement devrait garantir que les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil s'appliquent aussi aux utilisateurs finaux qui sont des personnes morales » et que « les personnes morales devraient avoir les mêmes droits que les utilisateurs finaux qui sont des personnes physiques en ce qui concerne les autorités de contrôle, lesquelles devraient aussi, en vertu du présent règlement, être responsables du suivi de son application relativement aux personnes morales ».

[24] Groupe de l'Article 29, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) du 4 avril 2017, WP 247, p. 9.

Dans le même temps, une disposition renvoie spécifiquement au Règlement d'une manière qui va potentiellement à l'encontre de cette interprétation de la portée du texte. Lorsqu'il est question de collecte d'informations sur un équipement terminal pour la connexion à un autre dispositif ou équipement, elle impose une obligation d'information si ces informations constituent des données à caractère personnel[25]. Il est alors renvoyé au RGPD[26]. Pourtant les bénéficiaires de la protection que prévoit cette disposition sont des utilisateurs finaux qui peuvent être des personnes physiques ou des personnes morales. En examinant le considérant qui contextualise cette obligation, on constate que l'hypothèse de départ est la collecte d'informations qui se trouvent sur des terminaux par des techniques de balayage des informations (pour le comptage de personnes, la fourniture de données sur le nombre de personnes dans une file d'attente, le calcul du nombre de personnes se trouvant dans un périmètre précis, pour reprendre les exemples cités). Il est donc question de recueillir des informations associées à l'utilisation d'un équipement par une personne physique et non au premier chef des données associées à une personne morale.

Il semble donc que, sauf spécification contraire dans le texte[27], lorsqu'il est question de dispositions protégeant des utilisateurs finaux, ceux-ci bénéficient de la même protection quant au traitement de leurs données de communications, et ce qu'ils soient des personnes physiques ou morales.

9. Quant à la l'application du RGPD à ces traitements, l'article 95 du RGPD prévoit que « [l]e présent règlement n'impose pas d'obligations supplémentaires aux personnes physiques ou morales quant au traitement dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union en ce qui concerne les aspects pour lesquels elles sont soumises à des obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE ». Si l'on doit déterminer dans quelle mesure des dispositions du RGPD trouvent à s'appliquer dans le contexte d'un traitement visé par cette directive, on doit se référer aux dispositions de cette directive.

---

[25] Voy. art. 8, § 2, de la Proposition de Règlement ePrivacy.

[26] Plus spécifiquement à l'article 13 du RGPD.

[27] Voy. l'article 15 de la Proposition de Règlement ePrivacy qui prévoit une protection spécifique uniquement pour les personnes physiques lorsqu'il est question d'insérer des données les concernant dans des annuaires publics.

À supposer que l'on puisse raisonner de même concernant le Règlement qui a vocation à remplacer la directive[28], on en déduit qu'il faut se fier aux dispositions du futur Règlement ePrivacy pour déterminer si et dans quelle mesure les dispositions du RGPD s'appliquent. La Proposition de Règlement ePrivacy n'offre pas de réponse explicite et distille dans les considérants et dispositions des allusions au RGDP sans dissiper toute ambiguïté concernant les personnes morales et le RGPD. Comme pointé précédemment, la Proposition de Règlement ePrivacy laisse entendre dans son troisième considérant que le RGPD bénéficiera aux personnes morales mais la question de savoir dans quelle mesure ce sera le cas reste ouverte.

En effet, le mélange des genres ne permet pas d'y voir tout à fait clair : on comprend que le RGDP bénéficiera aux personnes morales lorsque les dispositions du futur Règlement ePrivacy s'y réfèreront mais le texte ne reste pas sans ambigüité pour le reste. Il est spécifiquement question de l'application du RGPD dans le texte de la proposition de Règlement pour ce qui concerne les exigences en matière de validité du consentement, de mise en œuvre dans certains cas d'une analyse d'impact conformément à l'article 36 du RGPD, d'informations à fournir lors de l'accès ou du stockage d'informations sur un équipement terminal, ou encore de la compétence des autorités de contrôle pour le contrôle de l'application de la proposition de Règlement et l'imposition de sanctions en cas de violations du respect de celui-ci[29]. Ainsi, si le consentement des personnes morales peut être requis pour certains traitements de données, bénéficieront-elles également des droits des personnes concernées (droit d'accès, droit à la portabilité des données, …) ? Le texte n'offre pas de réponse explicite à cet question.

En outre, le renvoi pur et simple aux dispositions du RGPD dont les dispositions sont pensées comme bénéficiant à des personnes physiques n'est pas sans poser des difficultés. Le Groupe de l'Article 29 soulève la question du consentement expressément évoqué dans les considérants de la proposition de Règlement et pour lequel le RGPD fournit une définition inadaptée aux particularités des personnes morales[30].

[28] Ce que prévoit l'article 27 de la Proposition de Règlement ePrivacy.

[29] Voy. not. art. 6, § 3, 7, 8, 9, 18 de la Proposition de Règlement ePrivacy.

[30] Groupe de l'Article 29, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) du 4 avril 2017, WP 247, pp. 28-29).

CHAPITRE 3. Une approche moins sectorielle de la protection des données de communications électroniques

10. Si l'évolution qui se dessine en la matière nous éloigne d'une protection des données limitées à des personnes physiques, elle laisse présager de modifications quant aux services de communications électroniques concernés, par rapport au régime actuel.

Le futur Règlement ePrivacy devrait englober plus généralement les services accessibles au public, indépendamment du fait que le réseau utilisé est un réseau public ou privé. L'objectif avoué est de toucher les services d'accès au wifi fournis par des entreprises commerciales à des clients de passage par exemple[31]. Par ailleurs, le législateur européen affiche l'intention d'inclure des fournisseurs de services via le web dans la règlementation partant du constat que les services de *webmail*, de messagerie instantanée ou encore de « Voice over IP » remplacent aujourd'hui bien souvent d'autres modes de communications électroniques qui étaient l'apanage des fournisseurs de services de communications électroniques, tels que les opérateurs « télécoms » ou les fournisseurs d'accès à l'internet. Cela impliquerait, au niveau du secret des communications, que l'on ne ferait plus de différences entre un *e-mail* échangé entre deux employés et des messages échangés via *Whatsapp* ou *Messenger*, ou un service de messagerie personnel lié à un réseau social, par exemple[32].

Cela a une incidence sur les personnes censées respecter le règlement puisqu'on élargit le spectre des fournisseurs de services qui seront désormais soumis à la règlementation.

Cet élargissement de la protection me semble découler d'une préoccupation d'assurer un renforcement de la protection des données et contenu des communications, à tout le moins pendant la transmission[33]. L'article 5 de la Proposition de Règlement ePrivacy est libellé comme suit :

---

[31] Voy. consid. 13 de la Proposition de Règlement ePrivacy.

[32] Voy. consid. 1 et 11 de la Proposition de Règlement ePrivacy.

[33] Le considérant 15 de la Proposition de Règlement ePrivacy laisse entendre que la protection liée au secret des communications ne prévaudra que *durant la transmission* de la communication et cesserait lorsque l'acheminement serait achevé. Cela fait l'objet de critiques de la part du Groupe de l'Article 29 et du Contrôleur européen à la protection des données (Contrôleur européen à la protection des donnée, Avis 6/2017 sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement « vie privée et communications électroniques »), p. 17 ; Groupe de l'Article 29, Opinion 01/2017 on

« Les données de communications électroniques sont confidentielles. Toute interférence avec des données de communications électroniques, comme l'écoute, l'enregistrement, le stockage, la surveillance et d'autres types d'interception, de surveillance ou de traitement des données de communications électroniques, par des personnes autres que l'utilisateur final est interdite, sauf dans les cas où le présent règlement l'autorise ». Et la proposition de Règlement de prévoir ensuite des exceptions moyennant des garanties ou conditions supplémentaires pour certains traitements[34].

Il reste toutefois qu'on peut se demander s'il ne conviendrait pas, pour atteindre cet objectif, d'inclure d'autres personnes dans le champ d'application du futur Règlement.

Il n'y a pas de disposition précisant qui sont les destinataires primaires de la Proposition de Règlement ePrivacy. Seul le huitième considérant de la proposition liste les personnes auxquelles le Règlement est censé s'appliquer : « Le présent règlement devrait s'appliquer aux fournisseurs de services de communications électroniques, aux fournisseurs d'annuaires accessibles au public et aux fournisseurs de logiciels permettant des communications électroniques, y compris la récupération et la présentation d'informations sur Internet. Il devrait également s'appliquer aux personnes physiques et morales utilisant des services de communications électroniques pour envoyer des communications commerciales de prospection directe ou recueillir des informations qui concernent l'équipement terminal de l'utilisateur final ou qui y sont stockées ». Le texte de la proposition, tel que libellé, ne semble pas inclure tout « tiers » à une communication dans le champ d'application du Règlement. Le Contrôleur européen à la protection des données a d'ailleurs appelé à une clarification et estime que « [l]e traitement des données de communications électroniques et des informations liées aux équipements terminaux des utilisateurs devrait relever, sans ambiguïté, du champ d'application du règlement "vie privée et communications électroniques", *quelle que soit l'entité chargée de traiter ces mêmes données*[35] »[36]. On viendrait à une protection des données de communications électroniques plus indépendante du cadre règlementaire des services de communications électroniques qui a pour première vocation de réglementer qui peut offrir quels services à quelles conditions. En

the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) du 4 avril 2017, WP 247, p. 26). Il n'est pas exclu que ce point soit revu : on conçoit mal qu'un élément aussi essentiel de la portée de la disposition ne soit précisé que dans un considérant.

[34] Voy. en particulier les articles 6 et 8 de la Proposition de Règlement ePrivacy.

[35] Souligné par l'auteur.

[36] Contrôleur européen à la protection des donnée, Avis 6/2017 sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement « vie privée et communications électroniques »), p. 20.

termes de protection des données de communications électroniques, la préoccupation est davantage de définir des règles qui protègent les personnes concernées par ces communications par rapport à l'accès et l'usage qui est fait de ces données. Il est plus logique d'imposer des restrictions à tout qui traite de telles données et c'est d'ailleurs ce que tend à faire la Proposition de Règlement lorsqu'il est question de placer des cookies dans le terminal d'un utilisateur ou de lui adresser du spam : les règles définies s'appliquent à toute personne qui pose les actes visés, sans que cela ne soit limité aux fournisseurs de services de communications électroniques. La même préoccupation devrait être prise en compte lorsqu'il s'agit de garantir la confidentialité des données de communications. D'ailleurs, nombre d'acteurs qui traitent des données de communication ne sont pas des fournisseurs de services de communication : tel est le cas par exemple des entreprises qui fournissent des produits ou applications qui recueillent des données de géolocalisation pour fonctionner sans pour autant fournir de services de communication électronique.

11. Ensuite, il demeure qu'une difficulté traverse toute la règlementation qui ne me semble plus prise en compte dans la Proposition de Règlement ePrivacy. La distinction entre abonnés et utilisateurs finaux. On sait que lorsqu'une personne navigue sur Internet pour ne prendre que cet exemple, il s'agit le plus généralement d'une personne physique qui peut être distincte de l'abonné. Il est fréquent qu'un abonnement soit souscrit par une personne morale (une entreprise) ou une personne physique (un chef de famille) et utilisé par d'autres individus (travailleurs/membres de la famille). Il n'est donc pas toujours évident ni opportun de vouloir distinguer entre personnes physiques et morales pour cerner les droits des bénéficiaires de la protection. En revanche, le fait de déterminer qui doit recevoir quelle information et qui a accès à quelle information me paraît être davantage pertinent.

En effet, lorsqu'il est question de traitement des données de communications, il est logique qu'à tout le moins ce soit les personnes dont les données sont traitées qui soient informées des possibles utilisations, dont le consentement soit requis le cas échéant et qui se voient octroyer un droit d'accès. La directive 2002/58/CE opérait une distinction entre abonnés et utilisateurs. Cette distinction n'est plus reprise dans la Proposition de Règlement ePrivacy. Il n'y est plus que question que d'utilisateurs finaux, notion évoquée ci-avant et qui peut désigner tant les personnes morales que les personnes physiques qui font usage du service. Or, il est possible qu'un fournisseur de services soit confronté à deux types d'utilisateurs : un qu'il a identifié et qui est son client (l'entreprise abonnée) et des utilisateurs qui lui sont inconnus (membre du personnel ou clients d'une

entreprise qui utilisent les services de communication électroniques). Les dispositions de la proposition ne font aucune distinction alors que l'abonné et l'internaute sont tous les deux des utilisateurs finaux des services. Cela pourrait poser des problèmes d'application pratique des dispositions de la proposition de Règlement lorsque l'on exige une information ou un consentement préalable pour le traitement de données qui sont liés à l'utilisation d'un service potentiellement souscrit par une personne et utilisé par d'autres. Un abonné peut-il solliciter l'accès à toutes données de communications électroniques, quand bien même il ne serait pas partie à celles-ci ? Cette question est tout à fait pertinente dans le contexte d'une relation de travail vis-à-vis des communications électroniques d'un employé.

Par ailleurs, si l'on a égard par exemple à l'article 6, § 3, (x) de la proposition de Règlement ePrivacy, l'approche qui se dessine semble vouloir faire abstraction de la dimension fournisseur/client. Cette disposition prévoit que « [l]es fournisseurs des services de communications électroniques peuvent traiter le contenu de communications électroniques uniquement afin de fournir un service spécifique à un utilisateur final, si l'utilisateur ou les utilisateurs finaux concernés ont donné leur consentement au traitement de leur contenu de communications électroniques et si la fourniture du service ne peut être assurée sans traiter ce contenu ». Cela implique-t-il que l'on doive identifier tous les utilisateurs finaux ? C'est ce que laisse entendre le considérant 19 de la proposition de Règlement qui semble inclure toutes les parties à la communication…[37]

12. Il résulte de ces différents éléments qu'il est difficile à l'heure actuelle de se faire une idée précise du régime qui prévaudra lors de l'adoption du Règlement ePrivacy.

Une autre source d'incertitude provient du fait que le considérant 7 de la Proposition de Règlement ePrivacy laisse entendre, dans des termes quelque peu obscurs, que les États Membres pourront adopter des dispositions nationales sans expliciter concernant quels aspects du Règlement ni avec quelle marge de manœuvre, sinon un objectif de « permettre de préserver un équilibre entre la protection de la vie privée et des données à caractère personnel et la libre circulation des données de communications électroniques ». Il n'est donc pas exclu que des dispositions de droit

[37] « Le présent règlement prévoit la possibilité, pour les fournisseurs de services de communications électroniques, de traiter des données de communications électroniques en transit, avec le consentement éclairé de tous les utilisateurs finaux concernés. Par exemple, les fournisseurs peuvent proposer des services qui impliquent le balayage des courriels pour en supprimer certain matériel prédéfini ».

national soient maintenues ou adoptées, y compris concernant la question du secret des communications pour préciser davantage et mettre en œuvre les règles contenues dans la Proposition de Règlement.

CHAPITRE 4. Vers un droit à la protection des données de communications électroniques ?

13. Les critères dégagés en matière de protection des données ne sont pas toujours des plus praticables : est-il adapté de vérifier si une donnée spécifique peut ou non concerner une personne physique identifiée ou identifiable pour que la protection s'applique ? Il est raisonnable de penser que souvent on aura intérêt à appliquer le même niveau de protection pour les traitements de données intervenant pour les besoins du service, indépendamment du client concerné. S'il paraît logique et souhaitable que soit prévue une réglementation relative au traitement des données dans le secteur des communications électroniques, il me semble que l'on pourrait aller plus loin et consacrer une protection autonome qui appliquerait des principes de protection indifférenciés aux données de communications sans qu'il soit exigé de passer par le filtre de qualification de données à caractère personnel mais qui conserverait une distinction entre les utilisateurs de services et les souscripteurs à ces services.

Par ailleurs, ce droit pourrait être davantage centré sur le traitement des données de communications électroniques et toucher, pour ce qui concerne les garanties attachées à la confidentialité des communications, les responsables de traitements qui traitent de telles données sans être limités aux traitements mis en œuvre par des fournisseurs de communications électroniques.